

TRAVAUX PRATIQUE :

**Développer, Deloyer et Interagir avec un
contrat intelligent sur Ethereum**

À la fin de votre exercice, poussez le code du contrat intelligent sur votre projet github que vous devez créer avec le répertoire principale « Système distribué : Blockchain & Contrat intelligent ».

Lorsque vous avez terminé la quête, veuillez inviter le professeur dont l'identifiant est le suivant @cozcan à collaborer à votre compte github. Tous les fichiers (fichiers de configuration, code de contrat intelligent...) créés pour ce TP devront y figurer. Vous rédiger un rapport avec chacune des étapes, il faudra réaliser un imprime écran de chacune des étapes comme illustrer dans le TP ainsi que fournir le lien Etherscan de chaque transaction réalisée.

Les objectifs de votre TP :

1. Prise en main des outils Remix et Metamask
2. Développement du smart contract
3. Déploiement du smart contract
4. Interaction avec le smart contract

Rappel :

Il existe différents environnements de développement pour réaliser ce TP. Nous utiliserons uniquement l'outil IDE en ligne [Remix](#) et le portefeuille électronique Metamask sur votre navigateur Chrome ou Firefox.

	Functionalities	Remix	MyEtherWallet	Geth
1	Configure the Blockchain Network	-	-	+
2	Deploy a private Blockchain	-	-	+
3	Develop a smart contract	+	-	+
4	Compile a smart contract	+	-	+
5	Create a user account "Wallet"	+	+	+
6	Deploy a smart contract	+	+	+
7	Create the UI for interacting	+	+	+
8	Run the Node client	-	-	+
9	Interact with the smart contract	+	+	+
10	Monitor the execution	-	-	+

1. Prise en main des outils Remix et Metamask

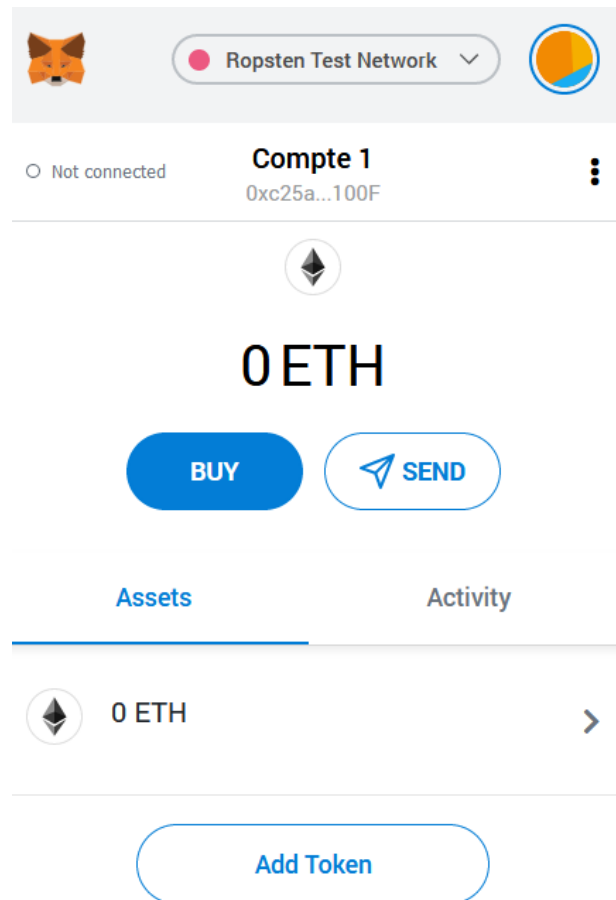
L'objectif de cette session est de prendre en main les outils permettant d'interagir avec une Blockchain de type publique.

Dans notre cas nous partirons sur une blockchain de type Ethereum et plus particulièrement sur l'environnement de test nommé « Ethereum Ropsten » permettant de pouvoir réaliser des transactions, déployer et interagir avec un smart contract gratuitement.

- a. Naviguer sur le site et télécharger Metamask sur le site suivant : <https://metamask.io/>
- b. Suivez les étapes de génération du portefeuille en sauvegardant bien votre seed

phrase

- c. Vous devrez ensuite avoir accès à votre premier compte « wallet » dont la clé publique commence par « 0x... » (voir illustration ci-dessous).



Vous disposez d'un compte avec zero ETH (Ether) qui représente la cryptomonnaie du réseau Ethereum. Afin de pouvoir réaliser des transactions et déployer un smart contract sur Ethereum il est nécessaire comme vu en cours d'avoir des ETH sur son compte.

- d. Recevez vos premiers ETH sur votre compte Metamask en allant sur la faucet en ligne en cliquant sur le bouton « Buy ».
- e. Consulter la transaction générée vers votre compte et prenez en compte les détails de cette dernière. Fournissez également les détails de la transaction

Transaction Details

Overview State

[This is a Ropsten **Testnet** transaction only]

Transaction Hash:	0x4ed61617f190d0afdc258b2b1f58e148bf9422d96a5a8b805632eae221cf57b
Status:	Success
Block:	8632651 5 Block Confirmations
Timestamp:	1 min ago (Sep-06-2020 08:47:42 PM +UTC)
From:	0x78c115f1c8b7d0804fbd3cf7995b030c512ee78
To:	0xc25a95a1d4a59a0e56f188f9c966a3dad518100f
Value:	5 Ether (\$0.00)
Transaction Fee:	0.00042 Ether (\$0.000000)

[Click to see More](#)

- f. Consulter ensuite le numéro de Block de votre transaction. Fournissez également les détails de la transaction

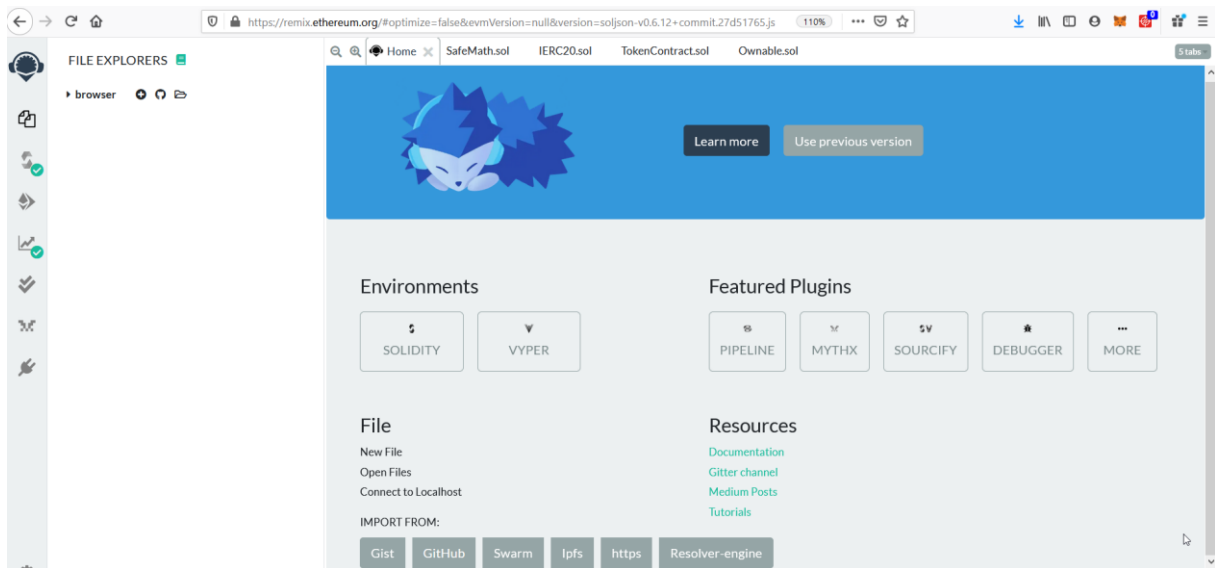
Block #8632651

Overview

[This is a Ropsten **Testnet** block only]

Block Height:	8632651
Timestamp:	4 mins ago (Sep-06-2020 08:47:42 PM +UTC)
Transactions:	6 transactions and 4 contract internal transactions in this block
Mined by:	0xad87c0e80ab5e13f15757d5139cc0c6fcb823be3 in 10 secs
Block Reward:	2.015309006321030221 Ether (2 + 0.015309006321030221)
Uncles Reward:	0
Difficulty:	444,313,161
Total Difficulty:	31,434,971,865,786,049
Size:	7,238 bytes
Gas Used:	1,444,273 (18.05%)
Gas Limit:	8,000,029
Extra Data:	020702/Parity-Ethereum/1.41.0/ (Hex: 0x0e830207028f5061726974792d457468657265756d86312e34312e30826c69)

- g. Générer votre première transaction Ethereum sur le réseau Ropsten envoyant 1 ETH à l'adresse suivante « 0xc25a95A1D4a59A0E56f188f9C966A3Dad518100F ».
- h. Ouvrir l'IDE Remix : remix.ethereum.org



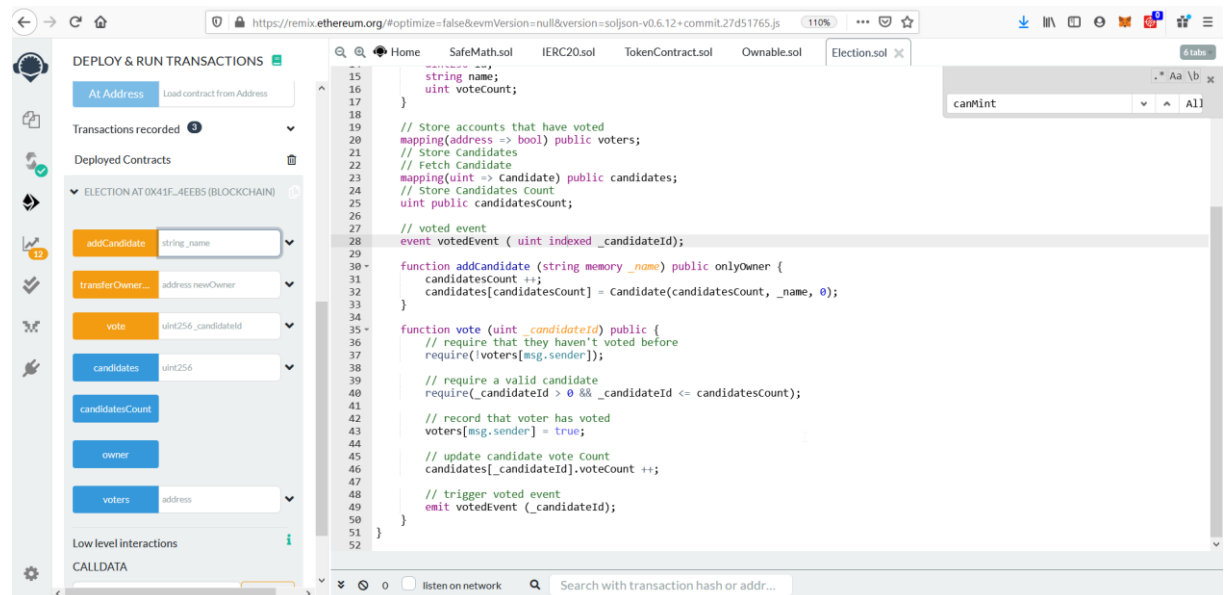
- i. Récupérer le code source de votre premier smart contract :
https://github.com/cozcan/TP_Election
- j. Ajouter l'ensemble des fichiers Solidity sur votre environnement Remix.
- k. Compiler votre smart contract « Election » et fournissez l'ABI ainsi que le Byte code du contrat.
- l. Déployer le smart contract « Election.sol » sur le réseau Ropsten et fournissez les détails de la transaction
- m.

Overview	State
① Status:	Success
② Block:	8632728 1 Block Confirmation
③ Timestamp:	40 secs ago (Sep-06-2020 09:05:48 PM +UTC)
④ From:	0xc25a95a1d4a59a0e56f188f9c966a3dad518100f
⑤ To:	[Contract 0x41fb182b28e5bb5410ce9c7d2167be663ff4eeb5 Created]
⑥ Value:	0 Ether (\$0.00)
⑦ Transaction Fee:	0.00244613438366 Ether (\$0.000000)
⑧ Gas Limit:	594,476
⑨ Gas Used by Transaction:	594,476 (100%)
⑩ Gas Price:	0.00000004114773992 Ether (4.114773992 Gwei)
⑪ Nonce	0 12
⑫ Input Data:	<pre> 0x608060405234801561001057600080fd5b50336000806101000a81548173fff021916908373ffffffff fff16021790555061096c806100606000396000f3fe608060405234801561001057600080fd5b506004361061 007d5760003560e01c8063462e91ec1161005b578063462e91ec146101835780638da5cb5b1461023e578063a3ec138d14610272578063f2fde38b14 6102cc5761007d565b80630121b93f146100825780632d35a8a2146100b05780633477ee2e146100ce575b600080fd5b6100ae600480360360208110 1561009857600080fd5b8101908080359060200190929190505050610310565b005b6100b861042f565b604051808281526020019150506040518091 </pre>

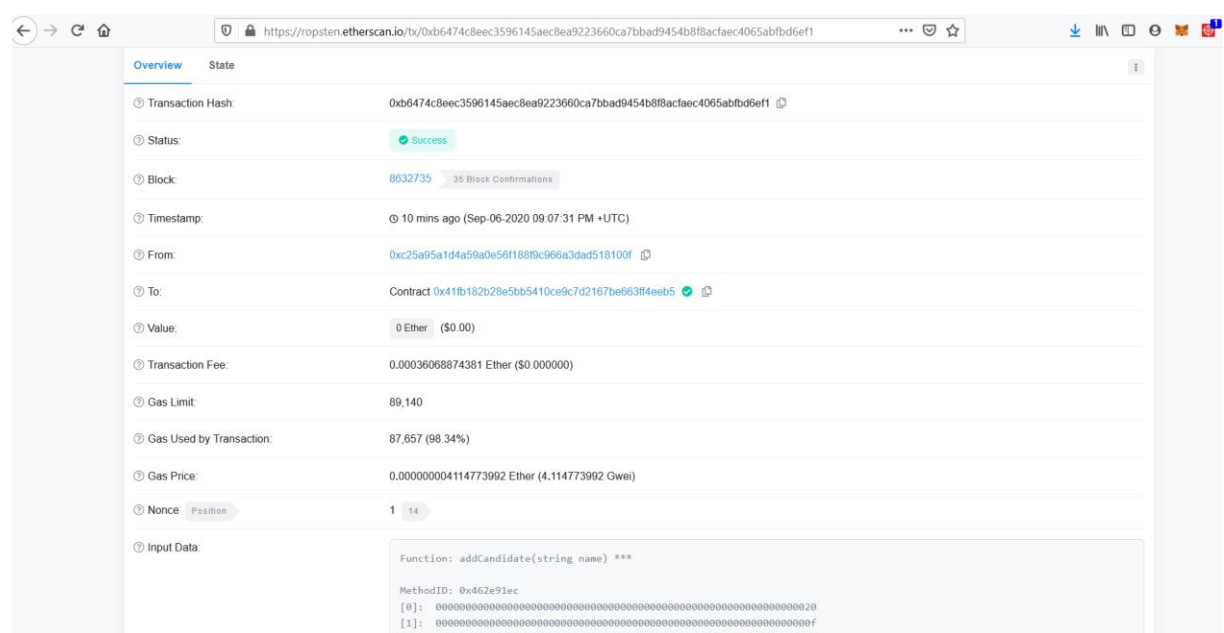
Justifier les frais de transactions « Transaction fees » que vous avez payés. Sont elles identiques à celle de ma transaction ?

Quelle est l'adresse public de votre smart contract ?

- n. Interagissez avec votre smart contract après l'avoir déployé en ajoutant le nom du premier candidat qui sera votre « Nom de famille »



- o. Générer la transaction ensuite l'ajout du premier candidat et fournissez les détails de la transaction



- p. Consulter la valeur de votre CandidateID à l'aide de Remix et fournissez le détail.
- q. Ajouter un second candidat de votre choix dans le smart contract et fournissez le détail de la transaction
- r. Consulter la valeur du second CandidateID à l'aide de Remix et fournissez le détail.
- s. Fournissez l'adresse du propriétaire du contrat
- t. Réaliser le premier vote pour l'un des candidats à travers Remix et fournissez le détail de la transaction
- u. Vérifier que votre vote a été prise en compte en fournissant la donnée du nombre de vote pour votre candidat.
- v. Demander à votre camarade proche de vous d'interagir avec votre contrat et de voter pour l'un des deux candidats en lui fournissant l'adresse publique de votre smart contract.
- w. Réaliser ensuite le transfert de la propriété à votre camarade en lui demandant son adresse publique.
- x. A votre avis comment pourrions nous sécurisé l'appel de la fonction addCandidate afin que vous soyez le seul à pouvoir gérer les candidats ?
- y. Modifier le code afin de faire en sorte que vous soyez uniquement le seul à pouvoir ajouter un nouveau candidat.